

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF NEW YORK**

---

**UNITED STATES OF AMERICA,**

**1:04-CR-340**

**v.**

**ABRAHAM PEARSON,**

**Defendant.**

---

**APPEARANCES:**

Kindlon and Shanks, P.C.  
74 Chapel Street  
Albany, NY 12207

Glenn T. Suddaby  
United States Attorneys Office  
James T. Foley U.S. Courthouse  
445 Broadway  
Albany, NY 12207

**OF COUNSEL:**

Terence L. Kindlon, Esq.

Thomas Spina Jr., Esq.  
Assistant United States Attorney

**THOMAS J. McAVOY,**  
**Senior United States District Judge**

**MEMORANDUM  
DECISION and ORDER**

**I. INTRODUCTION**

Defendant is charged in a multi-count Second Superseding Indictment with violations of Title 18, United States Code, Sections 2251(a) [Production of Child Pornography], 2252A(a)(1) [Distribution of Child Pornography], 2252A(a)(2)[Receipt of Child Pornography], 2252A(a)(5)(B)

[Possession of Child Pornography], and 2257 [Failure to Maintain Records]. Before the Court is Defendant's second omnibus motion<sup>1</sup> seeking (1) the dismissal of the Second Superseding Indictment based upon an alleged violation of the defendant's attorney-client privilege and destruction of exculpatory material, (2) the dismissal of counts 67-73 as multiplicitous, (3) the dismissal of counts 1-66 of the Second Superseding Indictment as legally insufficient under the Commerce Clause, (4) the suppression of physical evidence seized as a result of a search warrant executed on December 1, 2005, (5) the return of all property seized on December 1, 2005, (6) discovery, (7) the identification of all prior bad acts of Defendant, and (8) leave to make additional motions.

In addition, Defendant brings a separate motion seeking to quash a subpoena served upon him that requires him to produce at his trial "any and all passwords, keys, and/or log-ins used to encrypt any and all files" recovered on the computer drives and disks taken from his residence pursuant to a search warrant executed on December 1, 2005.

The Court will address these arguments seriatim.

## II. BACKGROUND

On June 13, 2003, Jane Doe # 2, then a 15-year-old female, informed members of the

---

<sup>1</sup> Defendant previously brought an Omnibus Motion. In a Memorandum-Decision and Order dated November 3, 2005, the Court ruled that Defendant's motion seeking: (1) dismissal of Counts 67, 69, and 70 as multiplicitous of Counts 1-66 and 68 was denied without prejudice to renewal at trial; (2) dismissal of Counts 1-66 as legally insufficient under the Commerce Clause was denied; (3) suppression of all physical evidence obtained as a result of a search warrant was denied; (4) in the alternative to suppression, an evidentiary hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978), was denied; (5) discovery pursuant to Rule 16 of the Federal Rules of Criminal Procedure was denied; (6) production of all Brady material was denied; (7) early production of Jencks material was denied; (8) identification of all prior bad acts of defendant the government intends to introduce at trial was denied; (9) preservation of law enforcement notes was denied; and (10) permission to make further motions was denied with the exception that "Defendant will be permitted to make additional motions only for good cause shown should additional discovery produce new material facts and issues."

Niskayuna Police Department (NPD) that Defendant was producing child pornography involving Jane Doe # 2 and Jane Doe #1, then a 17-year-old female. Fallon Aff. ¶ 3. In this regard, Jane Doe # 2 asserted that she and the other minor were paid to perform sexual acts with Defendant while he was filming them in his home at 2065 Orchard Park Drive, Niskayuna, New York. Id. The NPD obtained a New York State warrant to search Defendant's home and executed it on June 13, 2003. Id. Numerous items of evidence were seized, including computers, computer hard drives, and computer disks. Id. The computer disks allegedly contained hours of videos and still images of Defendant and Jane Does #1 and/or # 2 engaged in sexually explicit conduct. Id. Shortly after this discovery, the FBI became involved in the investigation. The investigation revealed that Defendant had labeled the disks in detailed fashion by date, volume, length, camera used, individuals appearing, and type of sexual activity. Id. ¶ 4. The FBI determined that on some disks or files, the individuals appearing in the videos and photographs were identified by code names. For instance, according to the Government the two Jane Does were, in some instances, both referred to as "SITGAL" ("Sitgal # 1" and "Sitgal #2") because both had been employed as babysitters for Defendant's children. Defendant referred to himself as "Ov" based upon his Hebrew name. Id. ¶ 4, 10(A).

The FBI also learned that Defendant sent, via the Internet, numerous images and movie files of Jane Does # 1 & # 2 engaged in sexually explicit conduct to David Gilinsky, Defendant's long-time friend who lived in Cleveland, Ohio. Id. ¶ 5. Gilinsky was interviewed and voluntarily turned over his computer to the FBI for analysis. Id. Sexually explicit images of Jane Doe # 1 were recovered from his computer. Id. Gilinsky also stated to the FBI that Pearson sent him numerous computer files from NY to Ohio via the Internet, and that the files contained sexually explicit

images of Jane Does # 1 & # 2. Id. Gilinsky asserted that Defendant told him that the girls were 17 years old. Id. Gilinsky later testified before a federal grand jury that returned a Superseding Indictment and a Second Superseding Indictment (discussed below). Id.

On February 16, 2004, Elijah Pearson, Defendant's father and an attorney admitted to practice law in the State of New York, wrote a letter to Glenn Suddaby, United States Attorney for the Northern District of New York. The letter appears to be a personal appeal to Suddaby regarding the prosecution of Defendant and includes the following passage: "I do not ask you for any favor. I do not participate or advise [Defendant]. He has a very good lawyer." Govt. Attach. G. At no time has Elijah Pearson entered an appearance in this case and, as early as the initial appearance on July 7, 2004, Defendant has indicated that he was represented by his current attorney-of- record, Terence L. Kindlon, Esq. See dkt. # 3.

On June 30, 2004, Defendant was indicted by a federal grand jury on one count of producing pornography based upon his alleged activities with Jane Doe #1. He was arrested on July 6, 2004, and released on bail. Upon his release, Defendant began residing at 4635 Slippery Rock Circle, Manlius, New York with his father, Elijah Pearson. Fallon Aff. ¶¶ 6-7. On February 11, 2005, Defendant was charged in a 71 Count Superseding Indictment with the production, transportation, possession, and receipt of child pornography, and with failing to keep individually identifiable records in violation of 18 U.S.C. §§ 2251(a), 2251(d), 2256(8), 2252A(a)(1), 2252A(a)(2), 2252(a)(5)(B), and 2257.

On November 29, 2005, the FBI received the results of a computer forensic examination conducted on the computer surrendered by Gilinsky. Fallon ¶ 8. The Government contends that this revealed that on multiple occasions between February 27, 2003 and May 27, 2003, Defendant sent

Gilinsky numerous sexually explicit images of Jane Doe # 1, as well as numerous e-mail messages. Id. During these exchanges, Defendant purportedly used one of two America Online email addresses - "Peall2065" and "Elijah1926." Id. America Online records showed that the "Peall2065" address was registered to Defendant, and the "Elijah1926" address was registered to Defendant's father. Id. ¶ 9.

Review of the email messages sent between Defendant and Gilinsky led the Government to believe that Gilinsky provided Defendant with sexually explicit images of Jane Does # 1 & # 2 after Defendant's home was searched and after he was arrested in June 2003. Id. ¶ 10. In addition, in an e-mail dated March 11, 2004 from "Peall2065" to Gilinsky's e-mail account, Peall2065 wrote:

To finish this morning's conversation: Ov will havem [sic] notebook at Binghamton meeting. Audio clips for analysis & manipulation could be crucial to Ov's defense. Remember SitGal # 2 is not legal. Ov has a "safe" for securing data & will change his password then so that no computer or human can retrieve saved data. The thing encrypts immediately (live/realtime) and will have a password like: eoKleGH93\*vfOY3Gw4kn&jd\$h. Also a shredder delete program is included to properly delete files &/or "free space". . . .

Id. ¶ 10(C).

The Government believed that this last e-mail indicated that Defendant was going to try to manufacture evidence that might exonerate him on the various charges, perhaps creating an audio or video file in which it appeared that the Jane Does represented that they were 18 years of age or older. Id. ¶ 18(b).

On November 20, 2005, the Government applied for a search warrant of Defendant's residence that he shared with his father, and of the computers in the residence, on the belief that Defendant had reacquired sexually explicit images of Jane Does # 1 & # 2. Id. ¶ 11. The warrant application was granted, authorizing the seizure of computers and computer related media that

might divulge evidence of the production, possession, receipt and distribution of visual depictions of minors engaged in sexually explicit conduct, including evidence of communications between Defendant, a.k.a. "Ov", "[Peall2065@aol.com](mailto:Peall2065@aol.com)", or "[Elijah1926@aol.com](mailto:Elijah1926@aol.com)", and Gilinsky (a.k.a. "dOv") at his America On Line account. Id.

The warrant was executed on December 1, 2005. Id. ¶ 12. At the time the warrant was executed, Defendant and his father were present. Id. ¶¶ 40-41. The Government contends that at no time did Elijah Pearson or Defendant represent that Elijah Pearson was representing Defendant, nor did government agents or attorneys have knowledge to that effect. Id. ¶¶ 36, 40-41; see Spina Aff. ¶ 29. Defendant has not presented any competent evidence to the contrary. The Government also contends that "at no time [on December 1, 2005] did Elijah Pearson or the defendant indicate that there were attorney-client materials or other privileged communications on either of the computers." Fallon Aff. ¶ 41. The Government concedes, however, that Defendant and his father represented to Government agents that Defendant used "his computer to research his case," and that "there would be research for other unrelated legal matters [of the father] on the computers." Id.

Pursuant to the search warrant, the Government seized, *inter alia*, (1) a 400 GB Sony Vaio Computer, Model PCV 1152, s/n 3000001; (2) a Sony Vaio Computer, model PCV-RX5500, s/n A8023273A 0204338; (3) a Western Digital external hard drive, s/n WCAEK1534T54; (4) a Sony thumb drive; (5) a Lexor thumb drive; and (6) over one hundred computer disks. Id. ¶ 12.

Other than the computer disks, this evidence was logged into evidence for analysis by a Computer Analysis Response Team (CART) agent, specifically trained in forensically analyzing computer media. Prior to analyzing any of the computer and computer media, mirror images were made.

Id. ¶ 13.

On Friday, December 2, 2005, the CART agent searched the computer media using the victims and Gilinsky's names. He recovered and printed out a multi-page typed document that he believed contained admissions by Defendant, and placed the document on Case Agent Fallon's desk. Id. ¶ 14. Fallon reviewed the document on the following Monday, December 5, 2005. Id. The CART agent was not in the office during the week of December 5, 2005 so Fallon could not ask where or in what file the document was found. Id. However, based upon review of the document, Fallon concluded that the document consisted of notes by Defendant about his case and contained what appeared to be an admission that he still possessed a computer disk containing sexually explicit images of the minors. Id.

\_\_\_\_\_Fallon also conducted his own search of the computer disks during the week of December 5, 2005 and discovered the following which he believed were relevant to the instant case:

(a) Four recorded telephone conversations between Defendant and Gilinsky. Each file had a ".wmv" extension, which led Fallon to believe that they were files similar to the sexually explicit images found on Gilinsky's computer (that were purportedly sent by Defendant), and included the name "Gilinsky" in the file name. Id. ¶ 15(a);

(b) Sixteen video files, two of which depicted unknown women stating that they were "18" and "18 and ½", respectively. Id. ¶ 15(b). Each file contained the ".wmv" extension, and were recovered from a disk labeled "BU Drive Easy Pass (X:) Case & Vid Editing Parts." Id. These were contained in a folder named "PRIVATE- For my Attorney-imp case files" and in subfolders named "ImpCaseData." Id. Fallon contends that he did not review the contents of any of the files in this folder except for the files that were identifiable as video folders by their size and ".wvm" extension. Id. Upon reviewing the two videos of the women stating their ages, Fallon formed the

opinion that they “were evidence of the defendant attempting to obstruct justice by manipulating the audio portions of the sexually explicit video tapes he has reacquired [from Gilinsky].” Id.

(c) A one page document containing two emails from Elijah Pearson to Gilinsky. Id. ¶ 15(c). In one email, a copy of which had already been recovered from Gilinsky’s computer, Elijah Pearson instructs Glinsky to erase evidence and discusses a possible interview with FBI agents. Id. The second e-mail also discusses a possible interview with FBI agents. The document was recovered from a disk labeled “Case B.U. 11-20-04”, found in a file named “PRIVATE-For my Attorney-imp case files” and in a subfolder entitled “Dov Warning before FBI.” Id. The file was named “emailfromEAPbeforedovFBIMeeting.jpg.” Id. Special Agent Fallon “believed it was appropriate to view this file since it appeared to be a communication with Gilinsky, which was covered by the terms of the search warrant.” Id.

\_\_\_\_\_The FBI also conducted a “limited forensic examination” of the 400 GB Sony Vaio Computer, Model PCV 1152, s/n 3000001. Id. ¶ 16. The “user” of the computer is identified in the computer’s registry as “CaptainOv,” leading the FBI to conclude that Defendant was the user since he had referred to himself as “the Captain” and “Ov.” Three image files were recovered from the computer depicting what appeared to the FBI to be images of the minor victims albeit not sexually explicit. Id. The FBI also found a number of encrypted files within a file labeled “steganosencryptionsafes,” but did not review any text files from this computer. Id.

\_\_\_\_\_A “very limited forensic examination” of the Sony Vaio Computer, model PCV-RX5500, s/n A8023273A 0204338 divulged (1) a file named “C:/Documents and Settings/HutUsers/Desktop/Excellent-FakeIDs ([Jane Doe #2]).htm”; and (2) an email dated March 18, 2004, from “steganos.asknet.de” to [“Peall20056@aol.com”](mailto:Peall20056@aol.com) in which “a password and serial



number necessary for downloading software capable of encrypting files were provided.” Id. ¶ 17.

The content of text documents from the computer were not reviewed, and the items recovered were not in files indicating that they may be privileged information. Id.

\_\_\_\_\_A forensic examination of the Western Digital hard drive revealed a “2.3 gigabyte encrypted folder/container.” Id. ¶ 18. Special Agent Fallon asserts “[a] file this size is large enough to contain a number of movie files and still images.” Id. However, the FBI is unable, at this time, to access the file to determine whether it contains any sexually explicit images of the minor. Id. The Western Digital hard drive did contain “files whose names appear to indicate that they contain privileged material” so these files were not reviewed. Id.

The Court’s file contains a letter written by Elijah A. Pearson to United States Magistrate Judge Randolph F. Treece. The letter is dated December 2, 2005 and was purportedly carbon copied to “Special Agent David Fallon; Judge Norman Mordue; Terrence Kindlon, Esq.; Thomas Spina, USA; and Rebecca Doyle, Pretrial Services.” The letter, which is stamped “received” by Judge Mordue’s Chambers on December 6, 2005, states in relevant part:

I was the subject of a search warrant on December 1, 2005. Both my computers were taken together with other materials.

I am an attorney working on my son’s case upon the computers which contained work product in his case and other legal matters.

I strongly believe the search was illegal and improper. It was an improper use of search and seizure of my legal material. Original exculpatory evidence was seized making a fair trial impossible at this point for defendant Abraham Pearson. All of the defense case strategy and information, totaling over 10 gigabytes of computer space, was taken....

The FBI believed that encrypted folders and files found on the various computers and computer media might have contained sexually explicit images of the minor victims. Id. ¶ 19.

Therefore, on December 7, 2004 the FBI sent the following items to the FBI's Cryptological and Electronic Analysis Unit: (1) a mirror image of the 400 GB Sony Vaio; (2) a mirror image of the Western Digital Hard Drive; (3) the Sony thumb drive; and (4) a computer disk labeled "Archive & B.U. 8/04" and which purportedly indicated that "it contains a long Steganos password." Id. The Cryptological and Electronic Analysis Unit has been instructed to try to access any encrypted files to determine whether they contain sexually explicit images of the minor victims, but not to view any text documents or potentially privileged material. Id.

\_\_\_\_\_ On December 12, 2005, Special Agent Fallon met with Assistant United States Attorney Thomas Spina. Id. ¶ 20; Spina Aff. ¶ 11. Fallon advised Spina of the various items that had been recovered from the computer thumb drive and the computer disks. Fallon Aff. ¶ 21; Spina Aff. ¶ 11. The first item presented to Spina was the multi-page typed document that Fallon believed contained an admission by Defendant that he still possessed computer disks containing sexually explicit images of one of the minor victims. Fallon Aff. ¶ 22; Spina Aff. ¶ 12; Govt. Ex. H. Spina noticed that the document "contained notes apparently written by the defendant about materials that could be used to impeach various witnesses and some legal research." Spina Aff. ¶ 12.<sup>2</sup> Upon reviewing the document, Spina inquired of Fallon regarding the source of the document. Fallon Aff. ¶ 22; Spina Aff. ¶ 12. Fallon purportedly responded that it was found on a thumb drive after a search for the name of the minor victims and the name "Gilinsky," but that he did not know the exact source and would check with the CART agent and advise by the end of the day. Fallon Aff. ¶ 22; Spina Aff. ¶ 12. Spina also was advised of or reviewed other potentially relevant information as follows:

---

<sup>2</sup> Spina provides a footnote in his affidavit indicating that the impeachment information in the document was already known to the Government. See Spina Aff. ¶ 12, n. 1.

(a) recorded telephone conversations between Defendant and Gilinsky, Spina Aff. ¶ 13; (b) the video files of the two unknown women stating that they are 18 and 18 ½, id. ¶ 14; (c) the two emails from Elijah Pearson to Gilinsky, id. ¶ 15; and (d) the file named “C:/Documents and Settings/HutUsers/ Desktop/Excellent-FakeIDs ([Jane Doe #2]).htm”; and the email dated March 18, 2004, from “steganos.asknet.de” to “[Peall20056@aol.com](mailto:Peall20056@aol.com)” in which a password and serial number necessary for downloading software capable of encrypting files were provided. Id. ¶ 16.

Later in the day on December 12, 2005, Special Agent Fallon advised AUSA Spina that the document containing what appears to be Defendant’s notes and the document containing e-mails from Elijah Person were “in folders whose names indicated that they may be privileged documents.” Id. ¶ 18. He indicated further, however, that the recorded telephone calls were from a separate computer disk which “was not labeled in the manner that would indicate that they were privileged.” Id. AUSA Spina sealed the document containing Defendant’s notes, instructed Fallon not to access any text documents on the computer media, and requested the FBI to create a “taint” team before conducting any further searches. Id. ¶ 20. Later that day, Spina advised Fallon “that the taint team should not view any materials seized on December 1, 2005, and that there should be no additional searches of the media.” Id. FBI’s Cryptological and Electronic Analysis Unit is still attempting to access encrypted files in order to determine whether they contain sexually explicit images of the victims, but have been instructed not to view “any text documents or potentially privileged material.” Id. ¶ 21.

The Government contends that:

Other than any sexually explicit images of the minors possibly contained in encrypted files and the videos contained in the “Case18Clips” folder, the government does not intend to introduce any evidence recovered during the December 1, 2005,

search at trial.

Id. ¶ 21.

On December 14, 2005, the Government re-interviewed David Gilinsky prior to his grand jury testimony that day. Id. ¶ 23; Gilinsky Aff. ¶ 10. Gilinsky's attorney was present during the meeting. Gilinsky Aff. ¶ 10. Spina mentioned to Gilinsky that Defendant had been recording his telephone calls, and discussed the emails from Elijah Pearson. Spina Aff. ¶ 24. Gilinsky was already aware that the FBI had recovered emails from Defendant indicating that Defendant had reacquired images of the two victims in the spring of 2004, and that indicated that Defendant might attempt to manipulate the videos. Gilinsky Aff. ¶ 11. AUSA Spina does not recall disclosing the existence or contents of any of Defendant's notes or the "Case18Clips" during this meeting. Spina Aff. ¶ 24. Gilinsky confirmed that he had provided sexually explicit images of the minor victim to Defendant after the originals had been seized by law enforcement. Spina Aff. ¶ 23; Gilinsky Aff. ¶ 12. Gilinsky also advised that Defendant had expressed an intention, *inter alia*, to manipulate the audio portions of these video tapes to make it appear that the minor victims stated that they were 18 years of age or older. Gilinsky Aff. ¶ 12. After the meeting, Gilinsky entered into a formal cooperation agreement and testified before the grand jury. Id. ¶ 13. Gilinsky asserts that he has never been asked or pressured by the Government to lie, and instead was advised repeatedly to "simply tell the truth." Id.

On January 11, 2006, a 74 count Second Superceding Indictment was returned. In addition to charging the same counts as the Superceding Indictment, it charged three new counts pertaining to Defendant's conduct in April 2004. See Second Sup. Indict. Counts 69 & 70 (charging separate violations of 18 U.S.C. §§ 2252A(a)(2) & 2256(8)); and Count 73 (charging a violation of 18

U.S.C. §§ 2252A(a)(5)(B) & 2256(8)). The government contends that all of the items seized on December 1, 2005, except the 2.23 GB encrypted folder contained on the Western Digital hard drive, have been returned to Defendant and that no information contained on the items seized was deleted or modified in any way. See Fallon Aff. ¶ 30.

On February 17, 2006, Defendant filed the instant Second Omnibus Motion. With that motion Defendant submitted an affidavit in which he attests that:

(2) My father, Elijah Pearson, . . . is one of the retained attorneys working on my case.

(3) Much of the material seized contained confidential attorney client files and communications kept on the seized computers.

(4) Much of the material seized constituted attorney work product, both by Elijah Pearson and by Kindlon and Shanks.<sup>3</sup> Key USA witness David Gilinsky has confirmed to me that the USA has used said attorney work product, conveyed in his discussion with prosecutor Spina. Mr. Gilinsky also told me that the government has pressured him to lie.

(5) Some of the material seized was exculpatory evidence, the loss of which severely prejudices me.

(6) The legal documents seized represent a large part of my trial strategy, and their loss severely prejudices me, both because said material is now in the hands of the government, and because I no longer have access to much of said material. Relevant files seized include about twenty interviews with several important witnesses and a statement by key USA witness, Mr. Gilinsky, on witnessing evidence altering by the FBI (none of which has been seen yet by Kindlon and Shanks).

---

<sup>3</sup> Defendant's counsel-of-record, Terence L. Kindlon, Esq., submits an affidavit that appears to contradict this assertion. Kindlon asserts:

19. Much of the material seized contained confidential attorney client communications and work product kept on the seized computers. According to Abraham Pearson the material included extensive notes by Elijah and Abraham Pearson on the planned cross examination of approximately twenty witnesses, including David Gilinsky. None of that particular material has been seen by the Office of Kindlon and Shanks, PC., and now it is in the possession of the government and the defense has no access to said material.

Kindlon Aff. ¶ 19 (emphasis added).

(7) Audio analysis and processing software for my defense was seized.

(8) All copies of finished media work product intended for trial, prepared with my attorney, Elijah Pearson, have been seized on December 1, 2005. ...

Pearson Aff. [dkt. # 50]. Gilinsky denies that he told Pearson that the Government had used “attorney work product,” and avers that he has not spoken to Defendant or Defendant’s father since December 5, 2005 (the day Gilinsky retained counsel). Gilinsky Aff. ¶ 15.

The Government’s opposition to the Second Omnibus Motion was sealed by order of the Hon. Norman A. Mordue, the District Judge originally assigned to this matter. On March 6, 2006, Judge Mordue recused himself from presiding over this case, and the case was re-assigned to the undersigned. See Order of Recusal [dkt. # 62]. On March 17, 2006, the Court received a letter from the Government which states as follows:

Dear Judge McAvoy:

I am writing to advise you that the prosecution of this matter has been reassigned to Jill Trumbull-Harris and Steve Grocki of the Department of Justice’s Child Exploitation and Obscenity Section. In addition, the FBI has reassigned the investigation to a special agent who was recently transferred to the Bureau’s Syracuse office from Baltimore. Special Agent Fallon and I will therefore not represent the government in this matter at trial. Rather, we will become, in effect, part of a “taint” team to ensure that the new attorneys and agent assigned are not exposed to any potentially privileged material. As a result, I will continue to represent the government on the current motions pending before the Court since they involve the allegedly privileged material.

Although reassignment of this matter is not required under the law inasmuch as there was no intentional review of privileged material and no inappropriate use of any such material, the government has taken these steps in an abundance of caution to eliminate any possible claim of prejudice to the defendant as the case moves forward.

Spina 3/17/06 Letter [dkt. # 67].

### III. DISCUSSION

#### A. Dismissal of Indictment based upon Violation of the Defendant's Attorney-Client Privilege

Defendant moves to dismiss the Second Superseding Indictment on the grounds that his Sixth and Fifth Amendment Rights were violated in obtaining this Indictment. He alleges that the Government improperly had access to, and used, materials protected by the attorney-client privilege and attorney work product in obtaining the Second Superseding Indictment. More specifically, he alleges that privileged information contained in computer media seized pursuant to the search warrant executed on December 1, 2005 was used to obtain the cooperation of a witness (Gilinsky) who testified before the grand jury on December 14, 2005. He further asserts that the computers and computer media contained exculpatory evidence which is now lost. In the alternative, Defendant seeks the dismissal of Counts 69, 70 & 73, which were added after the December 1, 2005 seizure.

On this motion, the Court will presume that Defendant's father is part of Defendant's defense team. Further, the Court will presume that, at the very least, Defendant's type-written notes constitute privileged material. See United States v. Defonte, — F.3d —, —, 2006 WL 623603, at \*3 (2d Cir. March 14, 2006)(holding that defendants handwritten notes of what he wanted to discuss with his attorney - and which he subsequently discussed with counsel - fit squarely within the scope of the attorney client privilege).

#### 1. Sixth Amendment

In determining whether there has been an intrusion into the attorney-client relationship in violation of a defendant's Sixth Amendment rights, Courts have examined the following factors: (1)

whether there was an intentional intrusion into the attorney-client relationship to gather confidential privileged information, or whether the intrusion was inadvertent; (2) whether evidence to be used at trial was obtained directly or indirectly by the government intrusion; (3) whether the prosecution obtained details of the defendant's trial preparation or defense strategy; and (4) whether the government, directly or indirectly, used or will use evidence obtained as a result of the intrusion to the substantial detriment of the defendant. Weatherford v. Bursey, 429 U.S. 545, 97 S.Ct. 837, 51 L.Ed.2d 20 (1976). The Second Circuit has held that "unless the conduct of the Government has ... been ... manifestly and avowedly corrupt, a defendant must show prejudice to his case resulting from the intentional invasion of the attorney-client privilege." United States v. Schwimmer, 924 F.2d 443, 447 (2d Cir.), cert. denied 502 U.S. 810 (1991)(citations omitted); United States v. Gartner, 518 F.2d 633, 637 (2d Cir.)(“Where, however, the conduct of the Government has not been so manifestly and avowedly corrupt, the courts have applied a different and less rigid rule which attempts to measure the harm or prejudice, if any, to the defendant rather than punish the prosecutor by freeing the defendant.”), cert. denied, 423 U.S. 915 (1975). Here, defendant cannot show manifest corruption, intentional invasion or actual prejudice

There is no evidence of manifest corruption by the Government in searching Defendant's residence and seizing the computers and computer media to which he had access. The search warrant was sought, and executed, based upon a demonstrated belief that there existed evidence of Defendant's continued violation of the child pornography laws at his residence and on the computers to which he had access. The uncontested facts indicate that at the time the Government executed the search warrant the Government had a legitimate reason for obtaining and executing the search warrant - namely, that Defendant had committed further crimes and a well founded belief that



the evidence of those crimes might be contained on the computers and computer media in his residence. This belief was founded upon evidence that the Government legitimately obtained from David Gilinsky's computer.

Further, there exists little if any evidence of intentional intrusion into the attorney-client relationship at the time the computers and computer media was seized and the FBI began its forensic evaluation of these materials. At the time the search warrant was issued and executed, there existed no evidence that Defendant's father was participating in his defense. Indeed, the father's letter to the United States Attorney claimed the opposite. There is no competent evidence before the Court that Defendant or his father made any representation to this effect before Defendant's handwritten notes were discovered and read by the FBI case agent. The FBI searched the computers and computer media by using search terms such as the victim's names or nicknames, and Gilinsky's name, or by looking for picture, video, or audio files that might be evidence of Defendant's further commission of child pornography-related crimes and otherwise avoided text material that might be privileged.

There is an indication, however, that shortly after the seizures, Defendant's father put the Government on notice that he was participating in his son's defense. Presuming that Elijah Pearson's December 2, 2005 letter reached the United States Attorney's Office the same day that it reached Judge Mordue's Chambers (December 6, 2005), the Government was on notice from that day forward that privileged material might be contained on the seized computer material. Even accepting this proposition, however, the Government's actions since December 6, 2005 have served to ameliorate any prejudice that might otherwise have befallen Defendant. AUSA Spina acted appropriately in sealing Defendant's notes upon reviewing them, see United States v. Weissman,

1996 WL 751386 \* 12 (S.D.N.Y. 1996)(Intrusion not intentional where AUSA had no idea what the file contained until information had fallen into his hands and he read the privileged memorandum), and creating a “taint team” to prevent the prosecution from gaining any advantage from the review of any potentially privileged material.

In addition, the Government indicates that it does not intend to offer any evidence from the December 1, 2005 seizure other than any sexually explicit images of the minors possibly contained in encrypted files and the videos contained in the “Case18Clips” folder. Sexually explicit images of minors (if they exist) and videos of women stating their ages do not constitute attorney-client material and, therefore, are not protected even assuming they were found in files marked “privileged,” “confidential,” or “attorney work product.” See United States v. Pelullo, 917 F. Supp. 1065, 1077 (D.N.J. 1995)(“While Pelullo may not have waived a privilege claim, the manner in which he packaged and warehoused his vast array of documents created conditions which negate his charge that the government deliberately seized documents which it knew to be privileged.”). Given the information tending to indicate that Defendant was contemplating manipulating the re-acquired videos of the minor victims, the “Case18Clips” folder is exempted from the protection of the attorney-client privilege under the crime-fraud exception. See In re John Doe, Inc., 13 F.3d 633, 636 (2d Cir. 1994).

Further, even assuming, arguendo, that there was an intentional violation of Defendant’s Sixth Amendment rights, there is no per se rule requiring dismissal of the indictment. “[A]bsent demonstrable prejudice, or substantial threat thereof, dismissal of the indictment is plainly inappropriate, even though the violation may have been deliberate.” United States v. Morrison, 449 U.S. 361, 364-65 (1981). In order to establish demonstrable prejudice, or the substantial threat

thereof, it must be shown at the very least that the confidential information was used for the benefit of the government or the detriment of the defendant. See United States v. Bishop, 701 F.2d 1150, 1156-57 (6<sup>th</sup> Cir. 1983)(actual use of notes by prosecutor drafted by defendant to his attorney, at his attorney's request, to cross-examine the defendant at trial constituted demonstrable prejudice). Mere exposure of the government to privileged materials is insufficient to warrant relief. See Schwimmer, 924 F.2d at 443 (“[M]ere ‘tangential [ ] influence ... [that privileged information may have on] the prosecutor’s thought processes in ... preparing for trial’ [is] not an unconstitutional use.”); cf. United States v. Riveccio, 919 F.2d 812, 815 (2d Cir. 1990)(To the extent government’s thought processes or questioning of witnesses were influenced by defendant’s immunized grand jury testimony, any such use was merely tangential and was not a prohibited use in the defendant’s prosecution); United States v. Noriega, 764 F. Supp. 1480, 1489 (S.D.Fl. 1991)(“Yet the simple fact of communication [of the privileged information to the prosecution] is insignificant for Sixth Amendment purposes if there is no gain to the prosecution or adverse impact on the defendant as a result.”).

The Second Circuit has noted that prejudice can be shown by establishing “that a prosecution witness testified concerning privileged communications, that prosecution evidence originated in such communication, or that such communications have been used in any other way to the detriment of the defendant.” United States v. Ginsberg, 758 F.2d 823, 833 (2d Cir. 1985). Yet, despite Defendant’s conclusory allegations to the contrary, there is no evidence that the Government used Defendant’s notes, or any other arguably privileged material seized on December 1, 2005, to convince Gilinsky to testify before the Grand Jury the second time. The recorded telephone calls with Gilinsky, and the emails from Elijah Pearson to Gilinsky, were not confidential

because they were communications with a third party. Further, the telephone calls were not contained in a file marked confidential, and were properly examined in the first instance to determine whether they were illegal video files. Once identified as telephone conversations with Gilinsky, it was permissible to listen to them to determine whether they contained evidence of the purported April 2004 exchange of child pornography.

Moreover, even had Gilinsky been told about privileged information, such indirect use is not prohibited. See Schwimmer, 924 F.2d at 446. At the time the government interviewed Gilinsky, it had recovered incriminating emails from his computer which indicated that he had provided Defendant with sexually explicit images of the minors after he was charged. Gilinsky had already been cooperating in the Government's investigation and had previously been interviewed and testified before a federal grand jury. Gilinsky's decision to testify on December 14, 2005 appears to be based upon the fact that the Government recovered evidence from *his* computer indicating that he provided Defendant with child pornography in April 2004, and that Gilinsky wanted to enter a cooperation agreement to protect himself. Still further, a review of the grand jury minutes reveals no indication that the Government relied on any arguably privileged material in its presentation to the Grand Jury, and there is no basis to conclude that the Government pressured Gilinsky to lie before the Grand Jury.

To the extent Defendant argues that the fact that the Government has read his alleged trial preparation notes constitutes impermissible "use", this claim is rejected. As indicated above, these notes have been sealed and the Government has created a taint team to prevent any impact upon the prosecution from these notes. Given the steps taken by the Government to protect the defendant from any prejudice arising from the review of protected material, Defendant's motion to dismiss the

Second Superseding Indictment, or any part thereof, on the grounds of a Sixth Amendment violation, is denied. See Singer, 785 F.2d at 234-35 (since district court's remedial measures were adequate, dismissal of Indictment was not required even where the government violated a defendant's sixth amendment rights by intentionally procuring and reviewing an attorney-client file and it was determined that such conduct threatened to create prejudice at a retrial).

## **2. Fifth Amendment**

Defendant's assertion that the computers and computer media contained exculpatory evidence and material to prepare his defense that is "now lost" appears to form the basis of his Fifth Amendment challenge to the Second Superseding Indictment. In order to obtain the drastic remedy of dismissing an indictment or reversing a conviction based upon a claim of governmental conduct in violation of the Fifth Amendment, "a defendant must establish that the government engaged in outrageous behavior in connection with the alleged criminal events and that due process considerations bar the government from prosecuting...." United States v. Cuervelo, 949 F.2d 559, 565 (2d Cir. 1991); see also United States v. Russell, 411 U.S. 423, 431-32, 93 S.Ct. 1637, 1642-43, 36 L.Ed.2d 366 (1973). The conduct must be so egregious that it simply shocks the conscience. See United States v. Rahman, 189 F.3d 88, 131 (2d Cir. 1999), cert. denied, 528 U.S. 1094 (2000). Dismissal of an indictment based upon such conduct is rare. United States v. Myers, 692 F.2d 823, 847 (2d Cir. 1982), cert. denied, 461 U.S. 961 (1983); United States v. Artuso, 618 F.2d 192, 196 (2d Cir. 1980). It has been noted that the power to dismiss a case on this basis should be used sparingly. United States v. Santana, 6 F.3d 1, 10 (1<sup>st</sup> Cir. 1993). "[T]he burden of establishing outrageous investigatory conduct is very heavy." Rahman, 189 F.3d at 131. "Such a claim rarely succeeds." United States v. LaPorta, 46 F.3d 152, 160 (2d Cir. 1994).

Defendant has not provided any particulars of the material that is now purportedly “lost,” and the Government has asserted that it returned, unaltered, all of the seized material other than the encrypted files. Thus, it may be that the encrypted files contain some type of “exculpatory evidence” or trial preparation material that Defendant now believes is lost. The Court finds that the best way to resolve this matter is to have the Defendant, his attorneys, and the Government’s “taint team” present during an *in camera* hearing at which time the Defendant will provide a more definite statement as to the particular location of the material he claims is lost, and the purported location of the material before the December 1, 2005 search. If the material is contained on the encrypted files and if the password is not otherwise required to be produced (see discussion below regarding Defendant’s Fifth Amendment challenge to the trial subpoena, infra), Defendant can choose to voluntarily provide the password for the file or files he contends contains exculpatory material and/or trial preparation material. The files will be reviewed in the presence of the participants to this hearing. If the material is exculpatory, it will be provided to Defendant and the taint team will be ordered not to divulge the information to the Government’s trial team. Under such circumstances, the Court will determine what remedy, if any, Defendant is entitled to. If Defendant asserts that there exists some other exculpatory evidence or trial preparation material other than which might be contained on the encrypted files, then he should be prepared to present evidence of this material at this hearing. The Government’s “taint team” will then respond to the arguments and/or factual assertions, and the Court will rule accordingly. The “taint team” will be ordered not to divulge to the trial team the nature of the alleged “lost” material.

Therefore, the Court reserves on Defendant’s Fifth Amendment challenge seeking dismissal of the Second Superseding Indictment. The hearing will be held immediately prior to trial.

**B. Dismissal of Counts 67-73 as Multiplicitous**

Defendant renews portions of his previous motion alleging that various counts of the indictment impermissibly charge him with the same offenses. As to the new counts contained in the Second Superseding Indictment, he argues that count 73, charging him with the possession of sexually explicit images of Jane Does # 1 & 2, should be dismissed since he is charged with receiving the same images in Counts 69 and 70.

For the reasons set forth in Judge Mordue's November 3, 2005 Decision on the same issue raised in the first Omnibus Motion, the motion is denied without prejudice to renewal at trial.

**C. Title 18, United States Code, Section 2251(a), Which Criminalizes the Production of Child Pornography, Is a Valid Exercise of Congressional Authority under the Commerce Clause.**

Defendant once again asserts that counts 1-66 of the Indictment should be dismissed because there are insufficient allegations that his activity substantially affected interstate commerce and, therefore, no federal jurisdiction exists. For the reasons set forth in Judge Mordue's November 3, 2005 Decision on the same issue raised in the first Omnibus Motion, the motion is denied.

**D. Suppression of Physical Evidence**

Defendant asks the Court to suppress all the physical evidence recovered from his residence pursuant to a search warrant on December 1, 2005 on the grounds that the evidence was seized in violation of Defendant's attorney-client privilege. In addition, Defendant asserts that since the affiant of the search warrant affidavit failed to inform the magistrate judge that the location to be searched was the law office of Defendant's father, all the evidence should be suppressed. In the alternative, the defendant seeks a Franks hearing on this issue.

In Franks v. Delaware, 438 U.S. 154, 98 S.Ct. 2674, 57 L.E.2d 667 (1978), the Supreme

Court ruled that in limited circumstances a defendant may be entitled to an evidentiary hearing concerning inaccuracies in an affidavit in support of a search warrant. To be entitled to such a hearing, a defendant must offer proof that statements in the affidavit are false and that the affiant made the false statement knowingly or with reckless disregard for the truth. United States v. Malsom, 779 F.2d 1228, 1235 (7th Cir. 1985); United States v. Rogers, 732 F.2d 625, 628 (8th Cir. 1984); United States v. Marcello, 731 F.2d 1354, 1358 (9th Cir. 1984). The defendant must also establish that without the allegedly false statement, the magistrate would not have issued the warrant. Franks 438 U.S. at 171-72; Malsom, 779 F.2d at 1235. Unless a defendant offers substantial proof that the affiant's statement was deliberately false or demonstrated reckless disregard for the truth, the defendant is not entitled to an evidentiary hearing. United States v. Phillips, 727 F.2d 392, 400 (5th Cir. 1984) (conclusory allegations insufficient to merit hearing); United States v. Reed, 726 F.2d 339, 341-42 (7th Cir. 1984) (self-serving statements not substantial preliminary showing required to obtain Franks hearing). Allegations of negligence or innocent mistake do not warrant an evidentiary hearing. United States v. Reed, 726 F.2d at 342; United States v. Cummings, 720 F.2d 927, 932 (6th Cir. 1983), cert. denied, 104 S. Ct. 2342 (1984). If a defendant fails to meet this threshold burden of providing substantial proof, the defendant's motion for an evidentiary hearing on this issue must be denied. United States v. Orozco-Prada, 732 F.2d 1076, 1089 (2d Cir.), cert. denied, 105 S. Ct. 154 (1984) (failure to present evidence supporting allegation that admittedly erroneous statements in affidavit were made intentionally or recklessly justified denial of Franks hearing).

Here, there exists no evidence that the Government agent made any false statements in his search warrant affidavit. As noted above, the Government was unaware that the defendant's father



was one of his attorneys. In addition, Magistrate Judge Treece, who signed the search warrant, was apparently aware that the defendant's father was an attorney since he had presided over Defendant's detention hearing and was told this information during this hearing. See Spina Aff. ¶ 32. One of the conditions of Defendant's release was that he reside with his father. In addition, Defendant's father had apparently written the magistrate judge prior to the issuance of the warrant and indicated that he was an attorney. Id.

Further, for reasons discussed above, there is no basis to suppress evidence on the claimed violation of the attorney-client privilege. The evidence that the Government intends to offer in this case from the December 1, 2005 search and seizure is not governed by the attorney client privilege.<sup>4</sup> Therefore, the motion to suppress and for a Franks hearing is denied.

**E. Request for the Return of Property**

Defendant alleges that the Government improperly seized privileged attorney-client material on December 1, 2005, and asks that "any and all property seized" be returned.

Rule 41(g) of the Federal Rules of Criminal Procedure provides:

A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to

---

<sup>4</sup> In its Memorandum of Law in Opposition to Defendant's Second Omnibus Motion, the Government contends:

At this time, the only evidence the government seeks to introduce from the items seized on December 1, 2005, are: (1) any sexually explicit images of minors involved (in the event they are located on the encrypted computer media), as direct evidence of reacquiring and receiving the images; (2) evidence that various files on computer media, including a 2.3 gigabyte file on an external hard drive, are encrypted, as consciousness of guilt; and (3) the "Case18Clips", as consciousness of guilt.

protect access to the property and its use in later proceedings.

Fed R. Crim. P. 41(g).

A Rule 41 motion may be denied “if the defendant is not entitled to lawful possession of the seized property, the property is contraband or subject to forfeiture or the government’s need for the property as evidence continues.” United States v. Van Cauwenberghe, 934 F.2d 1048, 1061 (9<sup>th</sup> Cir. 1991). Retention of evidence by the government is proper if the property is needed in an investigation or prosecution. Ramsden v. United States, 2 F.3d 322, 326 (9<sup>th</sup> Cir. 1993), cert. denied, 511 U.S. 1058 (1994); Sovereign News, 690 F.2d 569, 577 (6<sup>th</sup> Cir. 1982), cert. denied, 464 U.S. 814 (1983). According to the Advisory Committee Notes to the 1989 Amendment of Rule 41(e), “reasonableness under all the circumstances must be the test when a person seeks the return of property.” “However, ‘if the United States’ legitimate interests can be satisfied even if the property is returned, continued retention of the property would become unreasonable.’” Ramsden, 2 F.3d at 326 (quoting Advisory Committee’s Note to Rule 41). The burden is on the moving party to show that the seizure was illegal and that he is entitled to lawful possession of the property. Cauwenberghe, 934 F.2d at 1061.

The Court finds that under the circumstances, the search warrant was properly issued and the computers and computer media from Defendant’s residence were properly seized and searched. As indicated above, other than the Western Digital hard drive containing the 2.23 gigabyte encrypted folder, all of the items seized pursuant to the warrant have been returned to the defendant. See Fallon Aff. ¶ 30. However, copies of various items have been retained. Id. Some of these items have been retained because they contain encrypted media which may contain sexually explicit images of the minor victims. Id. The remainder have been retained purportedly to protect the

Government from claims by Defendant that evidence has been lost or destroyed. Id. The Government contends that, other than attempts to decrypt information to search for image files, no further searches of these items will occur.

Given the Government's representation, the fact that a taint team has been established by the Government, and that a pre-trial hearing will be held to determine the contents of the encrypted files, the motion is denied with leave to renew following the pre-trial hearing.

**F. Requests for Discovery**

Defendant has made a number of discovery requests which the Court will address seriatim.

Request (a) "All materials seized on December 1, 2005." The Government contends that the following material was seized on December 1, 2005: (1) a 400 GB Sony Vaio Computer, Model PCV 1152, S/N 3000001; (2) a Sony Vaio Computer, model PCV-RX550, s/n A8023273A 0204338; (3) a Western Digital external hard drive, s/n WCAEK1534T54; (4) a SONY thumb drive; (5) Lexor thumb drive; and (6) over one hundred computer disks. The Government further contends that other than the Western Digital hard drive, it has provided Defendant with all these items. In addition, except for the 2.3 gigabyte encrypted folder, the Government has provided Defendant with a copy of this hard drive. For the reasons discussed above, this disclosure by the Government is sufficient at the present time. After the pre-trial hearing, the Court will determine what, if any, additional discovery must be made.

Request (b) "All transcripts and/or copies of recordings or any and all audio/video tape recordings...." The government asserts that transcripts of any audio/video tape recordings are currently being prepared by the Government. The Government further asserts that transcripts will be provided to the defense once complete and that audio portions of these tapes have previously been

provided to Defendant. The Government further contends that the videos seized from Defendant's residences were made available to Defendant and he, in fact, viewed a number of them during a discovery conference. The Government represents that it will make the videos available to Defendant and any expert retained by Defendant. This disclosure is sufficient. The Government need not provide copies of the visual portions of computer videos that purportedly depict the actual production of child pornography. See United States v. Horn, 187 F.3d 781 (8<sup>th</sup> Cir. 1999); United States v. Kimbrough, 69 F.3d 723, 731 (5<sup>th</sup> Cir. 1995)(Rule 16 does not provide that child pornography, which is illegal contraband, can be distributed to, or copied, by defense); United States v. Husband, 246 F. Supp.2d 467 (E.D.Va. 2003).

Request (c) "any and all drafts of the transcripts, as well as all notes of the individuals preparing the transcripts." The Government asserts that, to the extent discoverable, any drafts of transcripts will be provided as Jenks Act material. This disclosure is sufficient.

Request (d) "all voice exemplars." The Government asserts that "at this time, there are no voice exemplars." Thus, there is no disclosure requirement for voice exemplars.

Request (e) "any and all records regarding the decision that this case be prosecuted federally." Defendant has provided no authority for this request. The Government argues that records regarding the decision that the case would be prosecuted federally, rather than in state court, are not discoverable. The Court agrees. This request appears to fall squarely within Fed. R. Crim. P. 16(a)(2) which exempts from disclosure "reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case." See United States v. Koskerides, 877 F.2d 1129, 1133 (2<sup>d</sup> Cir. 1989). Because the request specifically seeks materials concerning the decision to prosecute

this matter, the request is denied.

Request (f) “a complete designation of which recordings or portions thereof will be used ... at trial.” The government asserts that

[a]ll recordings and images created by Defendant and seized from his home which depict the two minors engaged in sexually explicit conduct will be introduced at trial. These items are more specifically set forth in the indictment by volume number. In addition, videos and still images depicting commercial child pornography will be introduced at trial. All these recordings and images and the others referred to in the indictment are available for inspection and review by the defendant. By letter dated July 22, 2004, the government informed the defendant that all the images were available for his review. Thereafter, the defendant viewed a number of these videos during a discovery conference.

Govt. Mem. L. p. 30. This representation is sufficient.

Request (g) “all court documents and transcripts related thereto.” It is not clear to the Court or the Government what Defendant is seeking in this request. See id. The Government represents that the New York State search warrants, applications and affidavits have already been provided to the defense, and documents and transcripts from this Court are available from the Court Clerk’s Office. The motion in this regard is denied.

Request (h) “all police reports.” Brady impeachment material (see Brady v. Maryland, 373 U.S. 83, 87 (1963)), as well as Giglio material (see Giglio v. United States, 405 U.S. 150, 154 (1972)), must be supplied to Defendant with the statements of witnesses producible under 18 U.S.C. § 3500(a) and (b) of the Jencks Act, which is to say these need not be produced until after the relevant witness has testified on behalf of the government. See United States v. McKenzie, 1996 WL 590730, at \* 3 (N.D.N.Y. Oct. 03, 1996)(citing United States v. Higgs, 713 F.2d 39, 44 (3d Cir. 1983)). It is the normal practice in the Northern District to require Jencks Act material to be handed over after the jury is selected for trial. To the extent that such material has not been handed over to

date, the Court can find no reason to depart from its usual practice and order early production.

**G. Identification/Preclusion of "Bad Act" Evidence**

Defendant has requested that the Court direct the Government to furnish evidence of all prior bad acts or similar acts of defendant which it will seek to have admitted at trial pursuant to Rule 404(b) of Federal Rules of Evidence. In addition, the defendant specifically seeks to exclude any prior bad acts.

In its prior motion response the Government identified prior bad acts it intends to introduce at trial. In addition, in subsequent correspondence, the Government identified additional "bad acts" evidence it intends to use. For the reasons stated in Judge Mordue's November 3, 2005 Decision, Defendant's motion is denied. Questions of admissibility of particular evidence will be addressed immediately prior to trial.

**H. Request for Leave to File Additional Motions**

Defendant will be permitted to make additional motions only for good cause shown. The Court will not, however, accept additional motions that rehash the issues presented in the current omnibus motion and will not grant leave to make additional motions based on information and legal arguments which could have been brought through the exercise of due diligence as part of the instant motion. The Court will exercise its discretion in determining the validity of any future motions. Accordingly, that part of the Omnibus Motion seeking leave to submit additional motion is **GRANTED** as set forth herein.

**I. Motion to Quash Trial Subpoena**

Defendant also moves to quash a subpoena issued in early 2006 which compels him to produce for the Government:

Any and all passwords, keys, and/or log-ins used to encrypt any and all files, including but not limited to, Steganos encrypted files, contained on the following items recovered from your residence pursuant to a search warrant on December 1, 2005, and currently in the government's possession:

1. A Western Digital hard drive, s/n WCAK 1534754;
2. A copy of a SONY Microvault USB flash drive;
3. A copy of a SONY Microvault USB flash drive;
4. A SONY vaio desktop computer, model PCU 1152, s/n/ A222663W;
5. A SONY DVD-R computer disk, labeled "Archive and BU 8/04."

Trial Subpoena, Govt. Ex. 1.

Defendant bases his motion to quash on two grounds. One, he asserts that his Fifth Amendment right not to be compelled to testify against himself protects him from having to produce the passwords. Two, he asserts that the files contain attorney-client privileged information to which the Government should not have access. For the reasons that follow, the Court will hold a factual hearing on this motion.<sup>5</sup>

The Fifth Amendment privilege against self-incrimination "protects a person ... against being incriminated by his own compelled testimonial communications." Fisher v. United States, 425 U.S. 391, 409 (1976); see U.S. Const., Amend. V ("No person... shall be compelled in any criminal case to be a witness against himself."). For a communication to be protected by the Fifth Amendment, it must be compelled, testimonial, and incriminating in nature. Fisher, 425 U.S. at 408. Failure to

---

<sup>5</sup>In a letter to the Court dated May 22, 2006, Defense Counsel asserts that the "trial subpoena issue [is] moot" because a recent newspaper article reported that "a law enforcement official close to the case said the FBI already has accessed the files but the agency is reluctant to testify about the methods it uses to crack encrypted files" due to national security concerns. Sprotbery 5/22/06 ltr & Ex. 1 [dkt. # 80]. The Court does not find that the pending motion is moot. While the information in the newspaper, if correct, might obviate the need for the subpoena (AUSA Spina has filed a letter indicating that the information in the newspaper is not accurate), the subpoena was issued by the Government. Until the Government withdraws the subpoena, it is still in effect. The motion to quash the subpoena was brought by Defendant, and the Court does not read Defendant's letter as an application to withdraw the motion or a concession that the motion to quash is moot because he has complied with the subpoena. If defense counsel is asserting that, under the circumstances, the refusal of the Government to withdraw the subpoena is an abuse of the subpoena power, then he should so state and be prepared to address the issue (with both factual and legal support) at the pre-trial hearing.

satisfy any of these three elements defeats the application of the Fifth Amendment privilege.

It is well-settled that "if the party asserting the Fifth Amendment privilege has voluntarily compiled [a] document, no compulsion is present and the contents of the document are not privileged." United States v. Doe, 465 U.S. 605, 612 n. 10 (1984)(Doe I); Fisher, 425 U.S. at 409-410 (Voluntarily produced documents are not compelled and, therefore, do not enjoy Fifth Amendment protection.). The Government argues that given the length and unrelated characters of the password, see Def. March 11, 2004 e-mail to Gilinsky ("The thing encrypts immediately (live/realtime) and will have a password like: eolKleGH93\*vfOY3Gw4kn&jd\$h. "), Defendant more than likely reduced the password to writing. Production of this voluntarily created writing would not, the Government argues, constitute compulsion. Defendant has not responded to this argument.

The Government also argues that the password itself is not incriminating, and therefore, Defendant has no Fifth Amendment privilege from producing it. Again, Defendant has not responded to the argument. Instead, Defendant argues that "[w]hile the *content* of the seized materials may not be protected by the Fifth Amendment because the production of said materials was not compelled or testimonial," the "act of producing the decryption information ... would violate the Fifth Amendment because it would 'communicate testimonial aspects as to the existence of the documents, possession or control of the documents, or the authenticity of the documents.'"" Def. Mem. L. in Supp. Mot. to Quash, pp. 1-2 (quoting In re Grand Jury Proceedings, 41 F.3d 377, 379 (8<sup>th</sup> Cir. 1994))(emphasis in original). This argument invokes the Fifth Amendment "act of



production” doctrine.<sup>6</sup>

The act of production doctrine was developed by the Supreme Court in a series of cases that addressed whether the act of producing otherwise unprivileged documents was protected under the Fifth Amendment’s self-incrimination clause. See Fisher, 425 U.S. at 409; Doe I, 465 U.S. at 612; Doe v. United States, 487 U.S. 201, 209 (1988)(“Doe II”); Baltimore City Dept. of Social Services v. Bouknight, 493 U.S. 549 (1990). The focus in such cases is on whether the act of producing the document (or some other thing sought) has “testimonial aspects” such as confirming the existence of an otherwise unknown incriminating document, establishing that the producer of the document had ownership or control of the document, or authenticating the document by establishing that the producer of the document believed that the document was what the subpoena requested. Doe I, 465 U.S. at 613; see also United States v. Hubbell, 530 U.S. 27, 36-37 (2000)(The “act of production” doctrine has been recognized as protecting individuals from incriminating themselves by being compelled to produce documents where the production could implicitly communicate incriminating facts, such as the admission that “papers existed, were in [the producing party’s] possession or control, and were authentic.”); In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993), cert. denied sub nom. Doe v. United States, 510 U.S. 109 (1994); United States v. Walker, 982 F. Supp. 288, 290-91 (S.D.N.Y. 1999)(The act of production doctrine applies to production of documents that are not themselves

---

<sup>6</sup> By proceeding directly to the “act of production” argument, Defendant essentially concedes that the password itself carries no Fifth Amendment privilege. See In re Hyde, 235 B.R. 539, 542-43 (S.D.N.Y. 1999)(“Our Court of Appeals has stated that the Fifth Amendment does not protect the contents of voluntarily prepared documents, either business or personal. Hyde has made no claim that the documents were not voluntarily prepared. The Bankruptcy Court, therefore, correctly determined that the contents of the books and records at issue are not privileged. Even if the contents of documents are not privileged, however, the act of producing those documents might be.”)(citing In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir.1993)).

privileged under the 5<sup>th</sup> Amendment but which may have some testimonial impact and an incriminating effect if produced.)(citing Doe I, 465 U.S. at 612).

However, where the existence, ownership, control, or authenticity of the document (or thing) is a “forgone gone” conclusion, the testimonial aspect of production is minimized if not eliminated. See Fisher, 425 U.S. at 411. As the Supreme Court noted in Fisher, production of already-known documents that “add little or nothing to the sum total of the Government’s information by conceding that he does have the papers” does not serve as a testimonial act deserving of Fifth Amendment protection. Fisher, 425 U.S. at 411; compare Hubbell, 530 U.S. at 44-45 (holding that where the Government had not demonstrated prior knowledge of the existence or location of 13,120 pages of documents produced, and where the subpoena made broad, general requests, the act of turning over those documents qualified as compelled, testimonial self-incrimination falling under the protection of the Fifth Amendment).

In the Second Circuit, “the act of producing [otherwise unprivileged documents] in response to a subpoena may require incriminating testimony in two situations: (1) if the existence and location of the subpoenaed papers are unknown to the government; or (2) where production would implicitly authenticate the documents.” In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d at 93 (citations and quotation marks omitted). Thus, “[t]he first prong in our Circuit's test for the act of production privilege asks whether the existence and location of the subpoenaed documents is known to the Government.” In re Hyde, 235 B.R. at 545 (citing In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d at 93. In this regard, the Second Circuit stated:

Production may not be refused if the government can demonstrate with reasonable

particularity that it knows of the existence and location of subpoenaed documents. Since Doe produced a copy of the calendar to the SEC and testified about his possession and use of it, its existence and location are “foregone conclusions,” and his production of the original “adds little or nothing to the sum total of the Government's information.”

In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d at 93(quoted Fisher, 425 U.S. at 411)(other citations omitted).

In the instant case, compliance with the subpoena does not tacitly concede the existence or location of the computer files because the files are already in the Government’s possession. Their existence is a foregone conclusion. Further, the Government has already concluded upon forensic examination that they are encrypted. The Government has also rightfully obtained information from Defendant indicating that he intended to encrypt certain files, and that Defendant was provided with encryption software. Thus, the existence and use of encryption software on the files recovered from Defendant is all but a foregone conclusion, and knowledge of the actual password adds little to what the Government already knows in this regard. The Government’s knowledge is sufficient to meet its burden to overcome the first prong of the act of production privilege. See Walker, 982 F. Supp. at 291-92 (and cases cited therein).

Under the second prong of this Circuit’s test, the Court “must next determine whether production would ‘implicitly authenticate’ the documents.” In re Hyde, 235 B.R. at 545. “Implicit authentication occurs when an individual who receives a [subpoena] demanding production of documents complies with the [subpoena] and thereby implicitly testifies that he owns or at least possesses the documents.” Walker, 982 F. Supp. at 292 (quoting United States v. Fox, 721 F.2d 32, 38 (2d Cir. 1983).

Even when production could constitute authentication, however (i.e., when “a

government official will one day be able to testify that he knows the documents in question belong to petitioner because petitioner produced them when asked," [ In re Subpoena Duces Tecum, 616 F. Supp. 1159, 1161 (E.D.N.Y.1985) ], production can be compelled "when the government can authenticate the documents without relying on any act by petitioner." Id.; see also [ In Re Grand Jury Subpoena Duces Tecum, 1 F.3d 87, 93 (2d Cir.1993) ] (authentication by other means negates claim of privilege).

Id.; see also In re Hyde, 235 B.R. 546 ("While invocation of the act of production privilege does not automatically mean that it applies, in those cases that did not hold production privileged, there were means of authenticating the documents other than directly through the production sought.").

Here, on first blush, it would seem that compliance with the subpoena would not demonstrate an element of ownership or control of the files beyond what the Government already knows. Indeed, Defendant has already voluntarily asserted under oath that the seized files contain *his* material. See Pearson Aff. ¶¶ 3-8 [dkt. # 50]. Yet, he has asserted in this same affidavit that some of the materials on the computers were prepared by his attorneys. See e.g. id. ¶ 8 ("All copies of finished media work product intended for trial, prepared with my attorney, Elijah Pearson, have been seized on December 1, 2005."). It is unclear whether Defendant asserts that any of the encrypted files were prepared by his attorneys, and, thus, whether production of the password could serve to implicitly authenticate all the encrypted files. Of course, to the extent that Defendant asserts that the encrypted files were prepared by his attorneys, Defendant would have no Fifth Amendment "act of production" argument against their disclosure (although he may have other grounds to prevent the disclosure of the information to the Government, discussed below) . See Fisher, 425 U.S. at 409-410.<sup>7</sup>

---

<sup>7</sup> In this regard the Court wrote in Fisher:

[T]he Fifth Amendment would not be violated by the fact alone that the papers on their face might

(continued...)

If Defendant asserts that some of the encrypted files were prepared by his father, production of the password would not serve to authenticate *all* the files protected by the password. However, production of the password would provide powerful evidence on the issue of authentication of the encrypted files that his father did not produce because it would provide a link in the chain of ownership and control of any incriminating encrypted files. See Hoffman v. United States, 341 U.S. 479, 486 (1951) ("The privilege afforded by the Fifth Amendment not only extends to answers that would themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime."). Given this potential, the burden falls on the Government to demonstrate means to authenticate the files other than through the act of producing the password. Accordingly, the Court will hold a factual hearing to address whether the Government can authenticate the files by evidence *other* than the production of the password.

Turning to Defendant's second argument to quash the subpoena, the Court finds that the asserted attorney-client privilege is an insufficient basis for the requested relief. The bald claim that the files contain attorney-client privileged material is not a basis to refuse production of the encryption password. At the pre-trial hearing, only the Government's taint team will be present

---

<sup>7</sup>(...continued)

incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications. Schmerber v. California [384 U.S. 757, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966)]; United States v. Wade, [388 U.S. 218, 87 S.Ct. 1926, 18 L.Ed.2d 1149 (1967)]; and Gilbert v. California [388 U.S. 263, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1967)]. The accountant's workpapers are not the taxpayer's. They were not prepared by the taxpayer, and they contain no testimonial declarations by him. Furthermore, as far as this record demonstrates, the preparation of all of the papers sought in these cases was wholly voluntary, and they cannot be said to contain compelled testimonial evidence, either of the taxpayers or of anyone else. The taxpayer cannot avoid compliance with the subpoena merely by asserting that the item of evidence which he is required to produce contains incriminating writing, whether his own or that of someone else.

Fisher, 425 U.S. at 409-410.

(along with Defendant and his trial team) so the Court can fashion an appropriate remedy if the files contain protected material. If Defendant desires to voluntarily produce a password for certain files, or if the Court rules that the password must be produced, the Court can then examine the files to determine whether any contain attorney-client privileged material. If they do, the Court will issue an appropriate order protecting Defendant's constitutional right to counsel and to a fair trial.

#### **IV. CONCLUSION**

For the reasons discussed above, Defendant's Second Omnibus Motion is **DENIED** in all respects *except*:

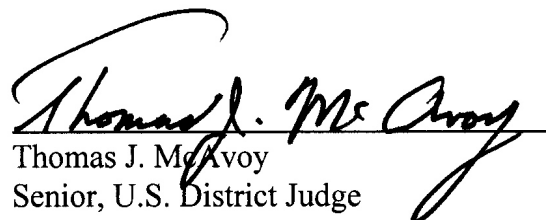
(a) to the extent that Defendant seeks to dismiss the Second Superseding based upon prosecutorial misconduct arising to the level of a Fifth Amendment violation, on which the Court **RESERVES** decision and will hold a pretrial hearing at which the Government's "Taint Team," the Defendant, and his lawyers will be present; and

(b) to the extent that this Decision and Order grants Defendant leave to make additional motions, or renew previous motions upon good cause shown.

Further, the Court **RESERVES** on Defendant's motion to quash the Government's subpoena, and will hold a pretrial hearing on this motion.

**IT IS SO ORDERED**

DATED: May 24, 2006

  
Thomas J. McAvoy  
Senior, U.S. District Judge